laptop computer; a vehicle; a car; a car key; a portable device; a handheld electronic device; and a single or multifunction device with cellular radio capability. The secure element may be removable or embedded or integrated in an existing processor architecture (e.g. baseband circuitry, main processor, central processing unit, and/or master control unit).

[0020] The cryptographic algorithms may be selected from a group consisting of MILENAGE; 128 bit TUAK; and 256 bit TUAK. The TUAK may refer to an algorithm set that complies with 3GPP TS 35.231 v. 12.0.1. The TUAK may be configured to employ AES cryptography. The TUAK may be based on Keccak permutation.

[0021] The authentication request message may be an extended authentication request message. The extended authentication request may comprise a message type indication that is configured to cause legacy terminals to neglect the extended authentication request message.

[0022] The extended authentication request may comprise a field configured to accommodate a 256 bit authentication token, AUTN.

[0023] The authentication token may comprise 128 bits, 192 bits, 256 bits or 320 bits. The authentication token may consist of 128 bits, 192 bits, 256 bits or 320 bits. In case that the authentication token is more than 256 bits, excess bits may be discarded.

[0024] The authentication token may comprise a sequence number, SQN. The sequence number may consist of 48 bits.

[0025] The authentication token may comprise an anonymity key, AK. The anonymity key may consist of 48 bits.

[0026] The authentication token may comprise an authentication management field, AMF. The authentication management field may consist of 16 bits. The authentication management field may comprise 7 spare bits. The spare bits may be used to indicate cryptography adaptation information. The cryptography adaptation information may comprise lengths of different cryptography parameters.

[0027] The authentication token may comprise a challenge, RAND. The challenge may consist of 128 bits.

[0028] The cellular authentication may employ a cipher key, OK. The cipher key may consist of 64 bits, 128 bits or 256 bits.

[0029] The cellular authentication may employ an integrity key, IK. The integrity key may consist of 64 bits, 128 bits or 256 bits.

[0030] The cellular authentication may employ a response parameter, RES. The response parameter may consist of 32 bits, 64 bits, 128 bits or 256 bits.

[0031] The authentication request message may be an updated authentication request. The updated authentication request may comprise an identifier for indicating which cryptographic algorithm is being used for the authentication. The identifier may be a new field in addition to those in the normal authentication request. The normal authentication request may comply with 3GPP TS 24.301 and 3GPP TS 24.008. Alternatively, the identifier may be contained in one or more bits of the authentication management field, AMF.

[0032] The authentication request message may comprise a protocol discriminator. The authentication request message may comprise a security header type. The authentication request message may comprise a non-access stratum key set identifier. The authentication request message may comprise a spare half octet. The authentication request message may comprise a challenge, RAND (e.g. evolved packet system, EPS, challenge). The authentication request message may comprise an authentication token, AUTN. The authentication token may comprise an authentication management field, AMF. The authentication management field may comprise a parameter indicating the length of TUAK to be used (e.g. 128 or 256 bit TUAK).

[0033] The message type may match with that of the normal authentication request message. The updated authentication request may comprise a 256 bit authentication token field. The updated authentication request may comprise a 256 bit authentication token field only if a 256 bit authentication token is being used. Otherwise, the updated authentication request may comprise a 128 bit authentication token field.

[0034] The authentication response message may comprise a message type indication. The message type indication may identify the authentication response message as an extended authentication response message. The message type indication may match with that of a normal authentication response message. The message type indication of the normal authentication response message may comply with 3GPP TS 24.301.

[0035] The extended authentication response message may comprise a variable length authentication response parameter, RES. The authentication response parameter may have a length selected from a group consisting of any one or more of: 32 bits, 64 bits, 128 bits or 256 bits.

[0036] The authentication response message may be provided with a new information element in comparison the normal authentication response message. The new information element may be configured to accommodate a 128 bit or a 256 bit authentication response parameter.

[0037] The authentication response message may comprise an extended authentication response parameter field that is configured to accommodate a 128 bit or a 256 bit authentication response parameter.

[0038] The authentication response message may comprise a cryptography algorithm indication.

[0039] The failure report may comprise an authentication failure message. The failure report may consist of an authentication failure message. The authentication failure message may comprise any of: a protocol discriminator; a security header type; an authentication failure message type; an EPS mobility management, EMM, cause; and an authentication failure parameter.

[0040] The cellular terminal may be configured to detect an error in a message authenticator of the authentication requests, MAC-A. The cellular terminal may be configured to produce the failure report in a manner dependent on the error that was likely to prevent successful decoding of the authentication request or the use of the selected cryptographic algorithm.

[0041] The cellular terminal may be configured to contain in the failure report, if the error was caused by incompatible length of MAC-A: an indication of the length of at least one of: the TUAK MAC-A used by the cellular terminal; and the TUAK MAC-A that the cellular terminal derives as likely used by the cellular network in the authentication request.

[0042] The failure report may comprise a new information element for error reporting. The error reporting may indicate a new EMM cause code. The error reporting may indicate an existing EMM code such as #20.